Meet the IDF-Linked Cybersecurity Group "Protecting" US Hospitals 'Pro Bono'

Anonymous "volunteers" from an opaque group founded by a former commander of Israel's Unit 8200 have been granted access to some of the most critical private and public networks in the US' healthcare and pharmaceutical sectors, with the help of a US federal agency now run by a former Microsoft executive.

BY **WHITNEY WEBB** AUGUST 27, 2020 19 MINUTE READ

audioread on rokfin

Since the Coronavirus crisis began in earnest earlier this year, the strain on hospitals in the US and around the world has been the subject of a considerable number of media reports. However, hardly any media attention has been given to the dramatic and unsettling changes that have been made to hospital and healthcare information technology (IT) systems and infrastructure under the guise of helping the US healthcare system "cope" with the surge in data as well as an unsettling uptick in cyberattacks.

Over the past several months, 80% of healthcare institutions in the US have reported being targeted by some sort of cyberattack, ranging from minor to severe, with an uptick in phishing attempts and spam specifically. Most of these attempts have been aimed at illegally acquiring troves of patient data, including the recent hacks of hospitals in Chicagoand Utah. About 20% of the hacks and cyberattacks

reported by hospitals and medical facilities since March directly affected the facilities' capacity to function optimally, with a much smaller percentage of those including ransomware attacks.

One of the reasons for the increase in the success of these attacks has been the fact that more healthcare IT workers are working remotely as well as the fact that many IT staffers have been laid off or let go completely. In several recent instances, the removal of entire hospital system IT staffs have been tied to a larger effort by the Department of Health and Human Services (HHS) to consolidate control over patient data, including Coronavirus-related data, with the assistance of secretive government contractors with longstanding ties to HHS.

The surge of cyberattacks combined with major budget cuts has made hospitals even more vulnerable as many are compelled to do more with less. As a result, there has been a renewed push for the improvement of cybersecurity at hospitals, clinics and other healthcare institutions throughout the country over the course of the Coronavirus (Covid-19) crisis.

Amid this backdrop, an odd group of "cyber threat intelligence" analysts with ties to the US government, Israeli intelligence and tech giant Microsoft have "volunteered" to protect US healthcare institutions for free and have even directly partnered with US federal agencies to do so. They have also recently expanded to offer their services to governments and social media platforms to target, analyze and "neutralize" alleged "disinformation campaigns" related to the Coronavirus crisis.

While these analysts have claimed to have altruistic motives, its members who have identified themselves publicly have notably dedicated much of their private sector careers to blaming nation states, namely Iran but also China, for hacking and, most recently, for cyberattacks related to the Coronavirus crisis, as well as the 2020 presidential campaign. These individuals and their employers rarely, if ever, make their reasons for assigning blame to state actors available to public scrutiny and also have close ties to the very governments, namely the US and Israel, that have been attempting to gin up hostilities with those countries in recent years, particularly Iran, suggesting a potential conflict of interest.

The Cyber Justice League?

Calling themselves the cyber version of "Justice League," the Covid-19 Cyber Threat Intelligence (CTI) League was created earlier this year in March and has described itself as "the first Global Volunteer Emergency Response Community, defending and neutralizing cybersecurity threats and vulnerabilities to the life-saving sectors related to the current Covid-19 pandemic." They now claim to have over 1,400 members hailing from 76 different countries.

According to their website, they seek "to protect medical organizations, public healthcare facilities, and emergency organizations from threats from the cyber domain" and offer their services "pro-bono" to major hospitals, healthcare and pharmaceutical companies as well as U.S. law enforcement and federal agencies. Upon their creation, they sent an "open letter to the healthcare community," offering to volunteer "their time and efforts to mitigate [cyber] threats and protect our healthcare system."

However, since its creation, the CTI League has offered its services to sectors entirely unrelated to healthcare systems, companies and institutions. For instance, they now offer their services to critical infrastructure systems throughout the US, including dams, nuclear reactors, chemical plants and others, according to their inaugural report and their contact form. This is particularly concerning given that there is no oversight regarding who can become a member of the League, as one must merely be approved for entrance or "vetted" by the league's four founding members, whose conflicts of interests and ties to the US and Israeli national security states are detailed later on in this report.

In addition, the league's team of "expert" volunteers also tackle alleged disinformation campaigns related to Covid-19. Some examples of the "disinformation" campaigns the CTI league has been investigating on behalf of its private sector and federal partners include those that "associate Covid-19 spread with the distribution of 5G equipment," "encourage citizens to break quarantine", and one that "incited" a "1st and 2nd amendment rally" in Texas.

Regarding their disinformation "workstream," the CTI league states the following:

"The CTI League neutralizes any threat in the cyber domain regarding the current pandemic, including disinformation. The mission of this effort is to find, analyze, and coordinate responses to the current pandemic disinformation incidents as they happen, and where our specialist skills and connections are most useful."

The CTI League has offered its services "pro bono" to a variety of groups in the private and public sector, which has allowed the League's members access to the critical systems of each. For instance, they work closely with the Health Information Sharing and Analysis Center (H-ISAC), whose members include Johnson & Johnson, Pfizer, Merck, Amgen, Blue Cross Blue Shield and Athenahealth, among others. H-ISAC's president, Denise Anderson, works closely with the National Cybersecurity and Communications Integration Center, part of the Department of Homeland Security (DHS). According to H-ISAC's Chief Security Officer (CSO), Errol Weiss, the organization has been partnered with the CTI League since "very early on" in the Coronavirus crisis.

The CTI League also works with unspecified law enforcement partners in the US and works particularly closely with the US Cybersecurity and Infrastructure Security Agency (CISA), an independent federal agency overseen by DHS. The current CISA director, Christopher Krebs – who was previously the Director of Cybersecurity for Microsoft, told *CSO Online* in April that "CISA is working around the clock with our public and private sector partners to combat this threat. This includes longstanding partnerships, as well as new ones that have formed as a direct result of Covid-19, including the Covid-19 Cyber Threat Intelligence (CTI) League."

Since they began "working with US authorities," the CTI League has increasingly taken to assigning blame to nation states, specifically Russia, China and Iran, for various cyber-intrusions just as the US federal authorities began to do the same. In late April, for instance, the Justice Department began claiming Chinese hackers planned to target "US hospitals and labs to steal research related to coronavirus" and anonymous US officials blamed China for a hack of the Department of Health and Human Services (HHS) and COVID-19 research. Yet, no evidence tying China to the hacks was provided and only anonymous government officials were willing to imply blame in statements given to the press, suggesting that there was not enough evidence to justify going public with the accusation or to even open an official investigation against specific foreign entities.

Notably, that same week in April, CTI League's founder Ohad Zaidenberg claimed that China, Iran and Russia "are trying to steal everything," telling *CBS News* that they "can steal information regarding the coronavirus information that they don't have, (if) they believe someone is creating a vaccine and they want to steal information about it. Or they can use the pandemic as leverage so they (can) to steal any other type of information."

Yet, upon looking more closely at the CTI league's membership and co-founders, particularly Mr. Zaidenberg, much of the league's leadership has a rather dubious track record regarding past claims linking state actors to cyberattacks. In addition, they also possess rather glaring conflicts of interests that undermine the CTI League's professed desire to protect critical health and other infrastructure "free of charge" as well as ties to foreign governments with a history of espionage targeting the United States.

ClearSky and the manufactured Iranian threat

The public face of the CTI League and its original founder is a young Israeli named Ohad Zaidenberg, who was previously an "award-winning" commander in Israeli military intelligence's Unit 8200, a key component of Israel's military intelligence apparatus that is often compared to the U.S.' National Security Agency (NSA). While serving in Unit 8200, Zaidenberg specialized in acts of cyberwarfare targeting the Iranian state, serving first as a Persian analyst in the Unit before becoming commander. His current biography states that he continues to remain "focused on Iran as a strategic intelligence target" and describes him as "an authority in the operations of key Iranian APTs [Advanced Persistent Threats]."

In addition to his leading role at the CTI League, Zaidenberg is also the lead cyber intelligence researcher at ClearSky Cybersecurity, an Israeli company directly partnered with the Unit 8200-linked Checkpoint and Verint Inc., formerly known as Comverse Infosys – a company with a long history of fraud and espionage targeting the US federal government. ClearSky also collaborates "daily" with Elta Systems, an Israeli state-owned subsidiary of Israel Aerospace Industries (IAI), and was founded by Boaz Dolev, the former head of the Israeli government's "e-Government" platform.

Aside from his work at CTI League and ClearSky, Zaidenberg is also a researcher for Tel Aviv University's Institute for National Security Studies (INSS). Zaidenberg is specifically affiliated with the INSS' Lipkin-Shahak Program, which is named after the former head of Israeli military intelligence and which focuses on "national security and democracy in an era of Post-Truth and Fake News." According to the INSS website, the program works directly with the Israeli government and the IDF and is currently headed by Brigadier General (Ret.) Itai Brun, the former head of the Israel Defense Intelligence (IDI) Analysis Division.

Prior to the creation of CTI League, ClearSky – and Zaidenberg, specifically – were often cited by US mainstream media outlets as the sole source for dubious claims that "Iranian hackers" were responsible for a series of high-profile hacks and "disinformation" campaigns. In every mainstream media report that has covered ClearSky's and Zaidenberg's claims regarding "Iranian hackers" to date, their connections to the Israeli government and Israeli intelligence services have been left unmentioned. Also unmentioned was the fact that the only state actor that ClearSky has ever blamed for hacks or other online attacks has

been Iran, suggesting that the government-linked cybersecurity firm has a rather myopic focus on the Islamic Republic.

Ohad Zaidenberg

For instance, in February 2018, *Forbes* reported on ClearSky's claim, citing only Zaidenberg by name, that an individual linked to Iran's government had been responsible for an "Iranian propaganda machine" producing "fake news" and attempting to imitate *BBC Persian*. Zaidenberg claimed that the individual behind the three "fake news" websites, which largely published criticisms of the *BBC* as opposed to false news stories, is "**believed** to have worked for [Iran's] National Ministry of Communications." Based merely on the Iranian national's "believed" (i.e. unconfirmed) work history, Zaidenberg then asserts with "medium-high certainty that the operation was funded by the Iranian government." Zaidenberg's history as a commander in Unit 8200 targeting Iran and his continued, self-admitted work in pursuing Iran as a "strategic intelligence target" while working at the Israeli government-affiliated ClearSky are left unmentioned by *Forbes*.

More recently, right before the founding of the CTI League, Zaidenberg and ClearSky were the sole source of claims that "Iranian hackers" were "exploiting VPN servers to plan backdoors" in companies around the world as well as targeting the networks of certain governments, mainly in the U.S. and Israel. ClearSky's assertion that the hackers in question were tied to Iran's government was solely based on their finding of "medium-high probability" that the hackers' activities overlapped with the past "activity of an [unspecified] Iranian offensive group." They declined to specify what the nature of the overlap was or its extent.

A clear conflict of interest

Notably, ClearSky's February report on "Iranian hackers" targeting governments and major international companies in the US and elsewhere came right on the heels of speculation that Iran would target the US with a cyberattack following the US' January assassination of Iranian general Qassem Soleimani, an act that was greatly influenced and allegedly prompted by Israeli intelligence. In the aftermath of the Soleimani assassination, mainstream media outlets in the US had heavily promoted the claim that Iran's government would soon respond with a "cyberattack" as retaliation and that"financial institutions and major American corporations may be in the crosshairs."

President Trump and Secretary of State Mike Pompeo had both threatened, at the time, to dramatically respond to any Iran-launched attack, including one launched in the cyber domain, presumably with military force. While Iran's much-hyped "cyber retaliation" failed to materialize, ClearSky, with its dubious claims that "Iranian hackers" were targeting major corporations and governments, created the impression that Iran's government *was* involved in cyberattacks against U.S. interests at this sensitive time.

ClearSky and Zaidenberg's claims regarding Iran only intensified after the CTI League was founded, with ClearSky and Zaidenberg being the only source for the claim made earlier this year in May that Iran had been responsible for the hacking of US biopharmaceutical company Gilead (a company which boasts close links to the Pentagon). The hack itself, which was widely reported by US media, is said to have consisted of a Gilead executive receiving a single "fake email login page designed to steal passwords" and it is unknown if the attack was even successful, per *Reuters*, which first broke the story in May. ClearSky subsequently claimed to have single-handedly "foiled" the Gilead hack. Notably, Gilead is part of H-ISAC, which had been partnered with Zaidenberg's CTI League weeks prior to the alleged hack.

The alleged Iranian-led hack received considerable media attention as the cyberattack was said to have targeted Gilead's antiviral medication remdesivir, which had received a Covid-19-related emergency use authorization from the U.S. Food and Drug Administration (FDA) just a week before the hack allegedly took place. Only Zaidenberg is cited by name in the report on Iran's alleged links to the Gilead hack, with *Reuters* citing two other, yet anonymous, cybersecurity researchers who told the outlet that they concurred with Zaidenberg's assertion "that the web domains and hosting servers used in the hacking attempts were linked to Iran."

Then, earlier this month, the FBI sent out a security alert claiming that Iranian government-aligned hackers were targeting F5 networking devices in the US public and private sector, with some media outlets citing anonymous sources tying the hackers in question to those previously identified by ClearSky. The FBI alert was issued right after an alert from CISA(which works directly with the CTI League and Zaidenberg) regarding vulnerabilities in F5 devices that did not mention the involvement of any state actors. Just a few days before the FBI alert, the director of the US intelligence community's National Counterintelligence and Security Center, William Evanina, had alleged that Iran was "likely" to use online tactics to "discredit U.S. institutions" and "to stir up U.S. voters' discontent."

Aside from citing only ClearSky and Zaidenberg for claims linking Iran's government to cyberattacks, it is also worth noting that the media reports that accused Iranian government-linked groups of committing those attacks declined to even mention the extreme extent to which Iran itself has been the subject of cyberattacks over the course of 2020. For instance, in February, a cyberattack took down an estimated 25% of Iran's internet, with some alleging US involvement in a similar attack that had targeted Iran just months prior. More recently, a series of several mysterious fires and other acts of industrial sabotage across Iran over the past few months have been linked to Israeli intelligence operations. In some cases, Israeli officials have acknowledged the Zionist state's role in these events.

In addition, there is the fact that top Israeli intelligence officials have attempted for years to goad the US into making the "first move" against Iran, both covertly and overtly. Indeed, for much of the last twenty years, Mossad has had access to "virtually unlimited funds and powers" for a "five-front strategy," involving "political pressure, covert measures, proliferation, sanctions and regime change" in order to target Iran. Some Mossad officials have openly stated that part of this "five-front" strategy involves directly influencing the US' Iran policy, including lobbying the U.S. to conduct a military strike on Iran. For instance, former Mossad director Meir Dagan, who pushed the US State Department to pursue "covert measures" and "urged more attention on regime change" in Iran while head of Mossad, is on record in 2012 stating that, in his view, the US needs to strike Iran first so Israel doesn't have to.

Currently, Israeli officials have been relatively candid about their role in several of the recent cyberattacks that have befallen Iran as well as the fact that powerful elements of the Israeli state are trying to get the US to join a conflict against Iran before the 2020 presidential election while Trump remains in power. The effort has reportedly led to concern among EU officials that Israel's government may be seeking to provoke an event whereby the US would engage Iran militarily.

This context highlights why solely citing a firm like ClearSky and an individual like Ohad Zaidenberg in linking a cyber attack to the Iranian government is dangerous, given that ClearSky and Zaidenberg's ties to the Israeli national security state presents a conflict of interest. This is especially true given that Zaidenberg's old unit in Unit 8200 is directly involved in conducting cyber attacks on Iran, like those that have been recently taking place as part of the strategy to provoke a military engagement between the US and Iran prior to the November elections.

While Iran's government could have been involved in recent cyberattacks, especially considering the extent to which Iran has been recently targeted by cyberwarfare, using a firm tied to the very government and military intelligence apparatus actively seeking to embroil the US in a war with Iran as the sole source linking Iran to a cyberattack is not only ill advised, but dangerous and reckless.

Furthermore, given Zaidenberg's key role in the CTI League, allowing faceless "volunteers" vetted by Zaidenberg and the league's three other founding members (whose affiliations are discussed below) onto critical private and public networks under the guise of "aiding" their security amid the Covid-19 crisis is similarly reckless.

CTI, Microsoft & 2020

While Zaidenberg has made himself the public face and spokesperson of the CTI League, it is worth examining the other three individuals that are listed as founding members on the League's website, if only because only these four individuals "vet" those who join the CTI League.

One of these other founding members is Marc Rogers, who began his career as a hacker and later "hacktivist" before deciding that "ethical hacking" was "more likely to have a positive outcome." For Rogers, "ethical hacking" meant pursuing a cybersecurity career with multi-national corporations like Vodafone and Cloudfare as well as asset management firms like Asian Investment & Asset Management (AIAM).

Rogers is currently the Vice President of Cybersecurity Strategy at Okta, an enterprise identity solution platform, co-founded by former Salesforce executives and largely funded by venture capital firm Andreessen Horowitz. Andreessen Horowitz is advised by former Secretary of the Treasury and Jeffery Epstein friend Larry Summers and is also a major investor in Toka, a company closely tied to Israel's military intelligence apparatus and led by former Israeli Prime Minister (and a close friend of Epstein's), Ehud Barak.

Aside from Rogers and Zaidenberg, the other founding members of the CTI League are Nate Warfield and Chris Mills. Warfield is a former self-described "Grey Hat" hacker (defined as "a hacker or cybersecurity professional who violates laws or common ethical standards but without malicious intent") who now works as a senior program manager for the Microsoft Security Response Center (MSRC). Mills also currently works for the MSRC as a senior program manager and he previously created the US Navy Computer Forensics Lab while serving in the Navy's Cyber Defense Operations Command.

The MSRC "proactively builds a collective defense working with **industry and government security organizations** to fend off cyberattacks" and works within the Cyber Defense Operations Center and Microsoft's other cybersecurity teams, including that previously overseen by Chris Krebs when he was in charge of "Microsoft's US policy work on cybersecurity and technology issues." Krebs, as previously mentioned, is now the head of the federal agency CISA, which oversees the protection of critical electronic infrastructure in the US, including the voting system. In addition to the above, MSRC is heavily focused on pursuing the cybersecurity needs of Microsoft customers, which includes the US government, specifically the US Department of Defense.

It is worth noting that the MSRC is also directly affiliated with Microsoft's ElectionGuard, a voting machine software program that was developed by companies closely tied to the Pentagon's infamous research branch DARPA and Israeli military intelligence Unit 8200 and creates several risks to voting security despite claiming to make it "safer." The push for the adoption of ElectionGuard software in the US has been largely spearheaded by the Chris Krebs-led CISA.

Perhaps more telling, however, is that Microsoft and the MSRC have been at the center, alongside ClearSky, of claims linking Iran's government to recent hacking events and assertions that Iranian government-linked hackers will soon target the US power grid and other critical infrastructure with cyberattacks. For instance, last year, Microsoft penned a blog postabout a "threat group" it named Phosphorus, sometimes also called APT35 or "Charming Kitten", and Microsoft claimed that they "believe [the group] originates from Iran and is linked to the Iranian government." Microsoft did not provide more details as to why they hold that "belief," despite the implications of the claim.

Microsoft went on to assert that the "Iranian" Phosphorus group attempted to target a US presidential campaign, which subsequent media reports revealed was President Trump's re-election campaign. Microsoft concluded that the attempt was "not technically sophisticated" and was ultimately unsuccessful, but the company felt compelled, not only to disclose the event, but to attempt to link it to Iran's government. Notably, the Trump campaign was later identified as the only major presidential campaign using Microsoft's "AccountGuard" software, part of its suspect "Defending Democracy" program that also spawned NewsGuard and ElectionGuard. AccountGuard claims to protect campaign-linked emails and data from hackers.

Though it provided no evidence for the hack or its reasons for "believing" that the attack originated from Iran, media reports treated Microsoft's declaration as proof that Iran had begun actively meddling in the US' 2020 presidential election. Headlines such as "Iranian Hackers Target Trump Campaign as 2020

Threats Mount," "Iran-linked Hackers Target Trump 2020 Campaign, Microsoft says", "Microsoft: Iran government-linked hacker targeted 2020 presidential campaign" and "Microsoft Says Iranians Tried To Hack U.S. Presidential Campaign," were commonplace following Microsoft's statements. None of those reports scrutinized Microsoft's claims or noted the clear conflict of interest Microsoft had in making such claims due to its efforts to see its own ElectionGuard Software adopted nationwide or the fact that the company has close ties to Israel's Unit 8200 and 8200-linked Israeli tech start-ups.

Coincidentally, Phosphorus, as Microsoft calls them, is also the group at the center of the "Iranian hacker" allegations promoted by ClearSky and Zaidenberg, which refers to this same group by the name "Charming Kitten." The overlap is not very surprising given Microsoft's long-standing ties to Israel's Unit 8200 as well as the fact that Microsoft as a company and its two co-founders, Paul Allen and Bill Gates, personally ensured the success of an Israeli intelligence-linked tech company then-led by Isabel Maxwell, Ghislaine Maxwell's sister who boasts close ties to Israel's national security state. It is certainly interesting that the four founding members of CTI League share ties to the same military intelligence agencies and associated corporations as well as an interest in the same group of alleged "Iranian hackers."

While CTI League only publicly identifies the names of its four founding members, further investigation reveals that another member of the league is its program lead for combatting Covid-19-related "disinformation" — Sara-Jayne Terp. Terp is a former computer scientist for the UK military and the United Nations and, in addition to her role at the CTI League, she currently co-leads the "misinfosec" (i.e. a combination of misinformation analysis and information security) working group for an organization known as the Credibility Coalition.

The Credibility Coalition describes itself as an effort to "address online misinformation by defining factors that communicate information reliability to readers" and is backed by Google's News Lab, Facebook's Journalism Project as well as Craig Newmark Philanthropies and the Knight Foundation. The latter two organizations also back the Orwellian anti-"fake news" initiatives called the Trust Project and the Microsoft-affiliated Newsguard, respectively.

Questionable access granted

Through claims of altruism and partnerships with powerful corporations and government agencies, the CTI League has been able to position itself within the critical infrastructure of hospitals and the U.S. healthcare system as well as attempting to expand into other key networks, such as those tied to dams and even nuclear reactors. It is truly stunning that a group whose unnamed members are "vetted" only by Zaidenberg, Warfield, Mills and Rogers, has been cleared to access critical private and public networks all because of the pandemonium caused by the Coronavirus crisis and the league's offering of their services "pro bono."

Notably, a considerable part of the strain that led hospitals and healthcare institutions to request the league's services, such as budget cuts or the firings of IT staffers, were actually the result of government policy, either due to state or federal budget cuts for healthcare systems or HHS' efforts to consolidate control over patient data flows into the hands of a few. In other words, these government policies directly led to a situation where hospitals and healthcare institutions would, out of desperation, be more likely to accept the "pro bono" offer of the CTI League than they otherwise would have been under more "normal" conditions.

Another critical fact worth pointing out is that the U.S. and Israeli intelligence communities have been seeding the narrative for over a year regarding the upcoming hacks of critical U.S. infrastructure on or around the US 2020 election, scheduled for November 3rd, by groups affiliated with the governments of Iran, Russia and/or China. As described above, many of the same groups and individuals behind the CTI League have played key roles in seeding aspects of that narrative.

Despite its massive conflict of interest, this opaque group is now nestled within much of the US' critical infrastructure enjoying little, if any, oversight – ostensibly justified by the league's "altruism." As a consequence, the group's opaqueness could easily lend itself to be used as the springboard for a "false flag" cyberattack to fit the very narrative pushed by Zaidenberg and his affiliates. From a national security perspective, allowing CTI League to operate in this capacity would normally be unthinkable. Yet, instead, this suspect organization is openly partnered with the US government and US law enforcement.

With US intelligence already having conducted such "false flag" cyberattacks through its UMBRAGE program, which allows them to place the "fingerprints" of Chinese, Russian and Iranian-affiliated hackers on cyberattacks that the U.S. actually conducts, any forthcoming cyberattack should be thoroughly investigated before blame is assigned to any state actor. Any such investigation would do well to first look at whether the CTI League was given access to the targets.

ClearSky COVID-19 cybersecurity Iran israel IT Unit 8200 US Hospitals

Author

Whitney Webb

Whitney Webb has been a professional writer, researcher and journalist since 2016. She has written for several websites and, from 2017 to 2020, was a staff writer and senior investigative reporter for Mint Press News. She currently writes for The Last American Vagabond.

32 comments

Occams says:
August 28, 2020 at 2:22 pm

”Since the Controlavirus Hoax began in earnest earlier this year, the strain on hospitals in the US and around the world has been the subject of a considerable number of media reports.”

There. Fixed it.

PS: The ‘strain’ was that the hospitals were empty, special facilities opened – then closed – with little to no patients. Talk to any nurse or doctor who is no longer afraid (they wouldn’t speak out at first) and they’ll tell you they’ve seen almost no hoax-patients, but REAL patients quietly sickened and died they were so terrified of the lies they were told they wouldn’t seek help.

And the entire medical industry went along with this hoax, but WERE nicely compensated for their collusion in the biggest fraud ever perpetrated.

And OF COURSE, if something stinks, is dirty, or harms America, our ‘best friend and ally’, Israel won’t be far away.
Reply

bright star says:
August 30, 2020 at 1:43 pm

Amen to that
Reply

Candide says:
August 29, 2020 at 11:13 pm

It seems everything bad in the world seems to lead back to Israel.
Reply

bright star says:
August 30, 2020 at 1:58 pm

If only more people knew how insanely dangerous these psychopaths are. But, since most people are not psychopaths, they are blind to that danger, until it is too late. Thank god that people like Whitney are doing their excellent work of trying to wake us up by writing awesome articles like this one.
Reply

Paul Smith says:
October 30, 2020 at 1:55 pm

Indeed
Reply

uncle tungsten says:
September 2, 2020 at 12:57 am

If CTI League does not document its work and the Health care institutions don't control those documents then the CTI League will be indispensable and the entire industry will be captured by this Trojan Horse. This is a brazen attempt to colonise the sector by an unaccountable and unimpeachable organisation. Only fools fall for this scam. That is why companies have IT people on staff and fully accountable and dependent. This CTI League scam reverses the dependency and will be fatal.
Reply

Luther Beckett says:
September 3, 2020 at 2:08 am

The revolving door relationships between IT companies, government, finance and healthcare was something I have personal experience with.

From what I can tell, Israel was embedded in American IT at least since the 1990s.

Microsoft's monopoly in government IT and Healthcare IT is ancient history – but interesting nonetheless. I went through the 'IT Consolidation in the early 2000s in Nashville. Within weeks after 9/11 we had 'spook' 'consultants' from companies like SAIC. Suddenly everything got corporate and militaristic at the same time. Can you say fascism? I suggest you do a search on 'CIA and SAIC'.

Windows is built with faults to allow 'back doors' – and they became the standard? There is a reason. It's because it CAN be easily exploited – but mostly kept under control by competent IT staff.

Nashville became a 'Microsoft Shop' because the city council was incompetent and bullied and MS had people embedded to break the rules about open bid contracts. I assume this is how they operated everywhere. I saw my boss go from Nashville Government to Microsoft to the US Department of Transportation to some company where almost everyone is ex CIA/NSA/Naval Intelligence, etc.

Helluva thing that needs undoing.
Reply

Nerdley Dorkmeister says:
September 5, 2020 at 10:43 pm

Is Whitney Webb the only legitimate journalist we have? It seems she is.
Fantastic Reporting
Reply

Bruce says:
October 30, 2020 at 2:12 am

Outstanding investigative reporting. No one does anything for "free" especially these very sophisticated Israeli IT specialists. Accessing medical data of Americans is but the proverbial foot in the door.
Reply

Paul Smith says:

October 30, 2020 at 2:15 pm

It’s always the Israelis with their ties to the “‘Deep State’”, criminal corporations, Media, and paid-off or blackmailed frequent flyer Congressmen covering for them. Trump just wants to be the hero with no regard for safety or ethicists of the C-Vaxx and his never ending ignorance on Israeli massive crimes and long term plans and ties to a Weaponized Covid vaccine. Trump trusting our worst enemy with every life in America and the world.
I wonder if Jews will be exempt from the C-Vaxx?
Reply